Notice of Allowability	Application No.	Applicant(s)	
	10/092,972	VANSTONE ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *09/29/06*.

2. ☒ The allowed claim(s) is/are *1-19*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *11/09/06* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Sean ZHang on 11/29/06.

The application has been amended as follows:

Claim 1 (Currently Amended). A method of authenticating a pair of correspondents A,B in a data communication system to permit exchange of information therebetween over a communication link, each of said correspondents having a respective private key a,b and a public key p_A, p_B derived from a generator α and respective ones of said private keys a,b, said method including the steps of

i) a first of said correspondents A selecting a first random integer x and exponentiating a function f(α) including said generator to a power g(x) to provide a first exponentiated function $f(\alpha)^{g(x)}$;

ii) said first correspondent A forwarding to a second correspondent B a message
including said first exponentiated function $f(\alpha)^{g(x)}$;

iii) said correspondent B selecting a second random integer y and exponentiating a function f(α) including said generator to a power g(y) to provide a second
exponentiated function $f(\alpha)^{g(y)}$;

iv) said second correspondent B constructing a session key K from information
made public by said first correspondent A and information that is private to said second correspondent B, said session key K also being constructible by said first correspondent A from information made public by B and information that is private to said first correspondent A;

v) said second correspondent B generating a value h of a function F[ð,K] where F[ð,K] denotes a cryptographic function applied conjointly to ð and K and where ð is a subset of the public information provided by B thereby to bind the values of ð and K;

vi) said second correspondent B forwarding a message to said first correspondent A including said second exponential function $f(\alpha)^{g(y)}$ and said value h of said cryptographic function F[ð,K];

vii) said first correspondent receiving said message and computing a session key
K' from information made public by said second correspondent B and private to said first correspondent A;

viii) said first correspondent A computing a value h' of a cryptographic function F[ð,K']; ~~and~~

ix) comparing said values obtained from said cryptographic functions F to confirm their correspondence[[.]]; and

x) upon such confirmation, permitting further exchange of information over said communication link.

Claim 11 (Currently Amended). A method of transporting a key between a pair of correspondents A,B in a data communication system to permit exchange of information therebetween over a communication link, each of said correspondents having a respective private key a,b and a public p_A, p_B derived from a generator α and respective ones of said private keys a,b, said method including the steps of

i) a first of said correspondents A selecting a first random integer x and exponentiating a function f(α) including said generator to a power g(x) to provide a first exponentiated function $f(\alpha)^{g(x)}$.

ii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function $f(\alpha)^{g(x)}$;

iii) said second correspondent B constructing a session key K from information
made public by said first correspondent A and information that is private to said second correspondent B, said session key K also being constructible by said first correspondent A from information made public by B and information that is private to said first correspondent A;

iv) both of said first correspondent A and said second correspondent B computing a respective value h,h' of function F[ð,K] where F[ð,K] denotes a cryptographic function applied to ð and K and where ð is a subset of the public information provided by one of said correspondents;

v) at least one of said correspondents comparing said values h,h' obtained from
said cryptographic function F to confirm their correspondence[[.]]; and

vi) upon such confirmation, permitting further exchange of information over said communication link.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100